daf MAGAZINE
Le magazine des directeurs administratifs et financiers
DAFMAG.FR
N°53
Automne 2022

LA COURSE AU CASH

LE DADA DU CREDIT MANAGER !

Les fraudes au paiement en hausse : pourquoi et comment limiter le risque ?

En 2021, une entreprise sur quatre a subi une fraude et pour un tiers, le préjudice dépassait 10 000 euros (Etude Fraude 2021, Euler Hermès /DFCG). Les fraudes au paiement sont les plus fréquentes. Les explications de Stéphanie Bombart, dg d'Exalog, éditeur de logiciels de gestion des paiements et de la trésorerie.

Fraude au faux-président, fraude au faux fournisseur ou au faux client : les fraudes au paiement sont les plus fréquentes car souvent les entreprises exposent leurs coordonnées bancaires et celles de leurs parties prenantes. Le risque cybercriminel est aussi porté par le conflit en Ukraine mené par la Russie selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

QUELS SONT LES CAS LES PLUS FRÉQUENTS OÙ UNE ENTREPRISE S'EXPOSE À DES FRAUDES AU PAIEMENT ?

STÉPHANIE BOMBART, DG D'EXALOG : d'abord, lorsque l'entreprise ne dispose pas d'une plateforme de gestion de paiements. Il lui faut donc se connecter sur le site de chaque banque pour procéder aux paiements. D'où des procédures d'authentification et de validation des paiements non homogènes et des coordonnées bancaires présentes sur plusieurs sites. Autre situation sensible : quand l'entreprise dispose d'un logiciel hébergé en interne. Les cyberattaques sont de plus en plus sophistiquées et très évolutives. Un éditeur spécialiste des flux financiers, qui s'occupera des infrastructures, des sauvegardes des données garantira une sécurité maximale. Dernière situation à risque : celle d'une forte digitalisation des processus sans formation et sensibilisation régulières des utilisateurs aux risques de fraude.

« Une seule et unique personne ne doit pas pouvoir effectuer toutes les étapes du paiement. »
STÉPHANIE BOMBART,
Directrice Générale d'Exalog

QUELLES SONT LES BONNES PRATIQUES INTERNES À DÉPLOYER PRIORITAIREMENT DANS LA GESTION DES PAIEMENTS ?

S. B : Opter pour la ségrégation des taches : une seule et unique personne ne doit pas pouvoir effectuer toutes les étapes du paiement. Ensuite, systématiquement vérifier toute modification des coordonnées bancaires d'un fournisseur, par exemple en l'appelant pour vérifier qu'il a effectivement changé de numéro de compte. Enfin paramétrer une liste blanche des pays où les paiements sont autorisés.

SI LE CHOIX EST FAIT DE DÉPLOYER UN OUTIL DE SÉCURISATION DES RELATIONS BANCAIRES, À QUOI LE DAF DOIT-IL VEILLER ?

S.B : Il doit s'assurer d'avoir la main sur le paramétrage des utilisateurs ; éviter les contrats reposant sur un coût par utilisateur ; s'assurer que l'application puisse être utilisée dans tous les pays (langue, fuseaux horaires, formats des dates et nombres) ; opter pour le mode Saas, synonyme d'agilité, de simplicité d'utilisation et de déploiement ; dernier aspect, porter attention à l'évolutivité du logiciel pour toujours être conforme aux bonnes pratiques de sécurité. Nos deux solutions Allmybanks, dédiée aux ETI et groupes avec des filiales et Exabanque qui adresse les PME, reposent évidemment sur ces paramètres.

OUTRE LA SÉCURISATION, QUEL EST L'AUTRE AVANTAGE D'UNE SOLUTION DE GESTION DES RELATIONS BANCAIRES ?

S.B : Des fonctions d'équilibrage et de centralisation du cash pour éviter les découverts ainsi que des outils qui simplifient l'enregistrement des prévisions pour anticiper les besoins en liquidités. Avantages qui parleront à toute fonction finance. ■

Exalog